

ISO/IEC 15408 Common Criteria Threat Categories

Purpose

This presentation introduces you to the threat categories contained in ISO/IEC 15408, used to assess the security level of products.

Not all threats can be handled programmatically.

However, by being creative and thinking outside the box, project teams can influence the outcome of almost all of them.

As you step through it, ask yourself:

“How can I handle, or influence the handling of this threat?”

Administrative Error of Commission

An administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application

- Accidental mismanagement of cryptographic functions
- Administrator error modifies access control or information flow policy
- Administrator error changes audit behavior
- Administrator error modifies authentication enforcement
- Administrator error makes information unavailable
- Administrator error makes resource unavailable
- Administrator error modifies entry policy
- Administrator error modifies user security attributes

Administrative Errors of Omission

The system administrator fails to perform some function essential to security

- Accidental mismanagement of cryptographic functions
- User privileges and/or authorizations are not updated upon reassignment
- Back door left open
- Administrator fails to update security configuration

Administrator Privacy Violation

An administrator learns the identity (or other privacy related information) of user(s) in violation of user privacy policy

- Administrator aggregates privacy information
- Administrator reads collected user privacy information
- Administrator reads system generated privacy information

Administrator Hostile Modification

An administrator maliciously obstructs organizational security objectives or modifies the system's configuration to allow security violations to occur

- Destruction or modification of audit data
- Administrator maliciously modifies or deletes data access control attributes
- Administrator modifies or destroys user data or applications
- Administrator maliciously modifies information flow control.
- Administrator maliciously modifies system entry parameters
- Administrator maliciously modifies security-critical code
- Administrator maliciously modifies user/subject bindings
- Administrator maliciously modifies user attributes and/or roles

Component Failure

Failure of one or more system components results in the loss of system-critical functionality

- Failure of external crypto support functions
- System hardware fails during system operation
- Resource depletion failure
- System use uncovers an intrinsic software flaw in a critical system component
- Accidental release of cryptographic assets due to Trusted Security Function flaw or malfunction

Data collection abuse

User abuses granted authorizations to improperly collect sensitive or security-critical data

- User collects data by browsing
- User collects authentication data by deception
- User collects data by deduction
- User collects data by eavesdropping
- User collects residual data

Data Smuggling

A user collects sensitive or proprietary information and removes it from the system

- User smuggles data using removable media
- Steganographic data smuggling

Denial of receipt

The recipient of a message denies receiving the message, to avoid accountability for receiving the message or to avoid obligations incurred as a result of receiving the message

- Denial of having received data from another local user
- Denial of having received information from a remote user
- Denial of having received information by a remote user

Denial of send

The sender of a message denies sending the message to avoid accountability for sending the message or to avoid obligations incurred as a result of sending the message

- Denial of having sent information to another local user
- Denial of having sent information to a remote user
- Denial of having sent data by a remote user

Denial of service attack

A hacker executes commands, sends data, or performs other operations that make system resources unavailable to system users. Resources that may be denied to users include bandwidth, processor time, memory, and data storage

- Hacker causes overload of communication resources
- Hacker causes system task overload resulting in denial of service
- Hacker activities cause storage overload

Distributed system component failure

Failure of a component that is part of a distributed system will cause other parts of the distributed system to malfunction or provide unreliable results

- Communications function failure

Eavesdropping

Hacker obtains user data by eavesdropping on communications lines

- The communication mechanism emanates data
- Outsider intercepts user communications
- An outsider taps a communications line

Encryption Hacking

A hacker performs cryptanalysis on encrypted data in order to recover message content

- Chosen ciphertext cryptanalysis
- Chosen plaintext cryptanalysis
- Chosen text cryptanalysis
- Ciphertext-only cryptanalysis
- Known plaintext cryptanalysis
- Hacker collects information via emanations analysis

Error invoked breach of confidentiality

A user commits errors that cause information to be delivered to the wrong place or wrong person

- Accidental or deliberate mishandling of cryptographic assets external to the product under development
- Under-classification of data sensitivity on export
- Accidental release of cryptographic assets due to user error
- Confidentiality violation of export control policy

Error invoked data inaccessibility

A user accidentally deletes user data or changes system data rendering user data inaccessible

- User error deletes data
- User error modifying attributes availability
- User error setting attributes availability

Error related breach of trusted security function

A user commits errors that cause the system or one of its applications to undermine the system's security features.

- Failure to provide object security attributes in data export
- Incorrectly set object attributes

Error related breach of data integrity

A user commits errors that induce erroneous actions by the system and/or erroneous statements its users

- Accidental or deliberate mishandling of cryptographic assets external to the product under development
- Falsification of information quality in data export
- User accidentally releases incorrect information
- User improperly modifies user data

Faulty Code

A system or applications developer delivers code that does not perform according to specifications or contains security flaws

- Inconsistent interpretation of audit data attributes
- Buffers not cleared by the system
- Incorrect modification of control data
- System data incorrectly exchanged
- Non-secure recovery
- Inaccurate system-data replication
- System modification by unauthorized source
- Malicious developer creates secret trapdoor in system
- Failure of external crypto support functions

Hacker undetected access

A hacker gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

- Hacker gains access through a vulnerability in code
- Weak system access control mechanism or system access control implementation

Malicious code attacks

An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of system assets

- Malicious code perpetrator dissemination
- Malicious code perpetrator execution
- Malicious code accidental IT download
- Malicious code IT execution
- Malicious code accidental user download
- Malicious code user execution

Man in the middle attacks (intercept & modification)

A hacker modifies information intercepted from a communication link between two unsuspecting entities before passing it on, thereby deceiving the intended recipient

- Modification of security-critical data in transit from a remote trusted site
- Modification of user data in transit from a remote site
- Modification of security-critical data in transit to a remote site
- Modification of user data in transit to a remote site

Masquerading

A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process

- A hacker assumes the identity of an authorized user
- A user assumes the identity of an authorized user
- Masquerading due to weak authentication

Misuse of available resources

A user's unauthorized use of resources causes an undue burden on an affected resource

- User's unauthorized use causes overload of communication resources
- Denial of service due to exhausted audit storage
- User obstructs legitimate use of resources.
- User's unauthorized actions over-task the system causing processor overload
- User's unauthorized actions cause storage overload

Non-repudiation controls circumvention

A participant in a transaction denies participation in the transaction to avoid accountability for the transaction or for resulting obligations

- Circumvent non-repudiation in a transaction involving a user and a local system
- Circumvent non-repudiation in a transaction involving a local user and a remote system
- Circumvent non-repudiation in a transaction involving a remote user and a local system

Physical System Attacks

- A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.
- Emissions interference
- Hacker collects information via emanations analysis
- Physical attack on cryptographic assets
- Hacker physically attacks the system

Power supply attacks

A human or environmental agent disrupts power causing the system to lose information or security protection

- Unexpected power reset

Social Engineering

A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation

- Social engineering to steal password
- Hacker uses social engineering to learn system information

Spooftng

An attacker tricks users into interacting with spurious system services

- Login program replicated to capture authentication data
- Attacker modifies protocol headers

Unauthorized modification

A user abuses granted authorizations to improperly change or destroy sensitive or security-critical data

- User modifies audit trail
- User improperly modifies authentication data
- User improperly modifies user data
- User improperly modifies Trusted Security Function data

User transmission abuses

A user abuses granted authorizations to improperly send sensitive or security-critical data

- Steganographic data smuggling
- User sends data violating confidentiality
- User sends data violating integrity



QualityIT™

Visit our resource site for more
security process tools and
information

<http://www.securityprocessprofessional.com>

Bar Biszick-Lockwood cisa, cissp, csqa,
206-388-3333 barbis@qualityit.net



<http://www.qualityit.net>